

(iv) The information is of a type not customarily in the public domain.

(b) Information that is not submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees will not qualify for protection under the CII Act of 2002. Any DHS component other than the IAIP Directorate that receives information with a request for protection under the CII Act of 2002, shall immediately forward the information to the Protected CII Program Manager. Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt and validate Protected CII pursuant to § 29.6(a).

(c) Federal agencies and DHS components other than the IAIP Directorate shall maintain information as protected by the provisions of the CII Act of 2002 when that information is provided to the agency or component by the Protected CII Program Manager or the Protected CII Program Manager's designees and is marked as required in § 29.6(c).

(d) All submissions seeking Protected CII status shall be regarded as submitted with the presumption of good faith on the part of the submitter.

(e) Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

#### **§ 29.6 Acknowledgment of receipt, validation, and marking.**

(a) *Authorized officials.* Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt of and validate information as Protected CII.

(b) *Presumption of protection.* All information submitted in accordance with the procedures set forth herein will be presumed to be and will be treated as Protected CII from the time the information is received by DHS, either through the DHS component or the Protected CII Program Manager or the Protected CII Program Manager's designees. The information shall remain protected unless and until the Protected CII Program Manager or the

Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

(c) *Marking of information.* In addition to markings made pursuant to § 29.5(a) by submitters of CII requesting review, all Protected CII shall be clearly identified through markings made by the Protected CII Program Manager or the Protected CII Program Manager's designees. The Protected CII Program Manager or the Protected CII Program Manager's designees shall mark Protected CII materials as follows: "This document contains Protected CII. In accordance with the provisions of 6 CFR part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protected CII Program requirements."

(d) *Acknowledgement of receipt of information.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall acknowledge receipt of information submitted as CII and accompanied by an express statement and certification, and in so doing shall:

(1) Contact the submitter, within thirty calendar days of receipt, by the means of delivery prescribed in procedures developed by the Protected CII Program Manager or the Protected CII Program Manager. In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the Protected CII Program Manager or the Protected CII Program Manager's designees of a written statement, certification, and documentation of the oral submission, as referenced in § 29.5(a)(3)(ii);

(2) Maintain a database including date of receipt, name of submitter, description of information, manner of acknowledgment, tracking number, and validation status; and

(3) Provide the submitter with a unique tracking number that will accompany the information from the time it is received by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(e) *Validation of information.* (1) The Protected CII Program Manager or the

## § 29.6

## 6 CFR Ch. I (1–1–05 Edition)

Protected CII Program Manager's designees shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Protected CII Program Manager or the Protected CII Program Manager's designee shall review the submitted information as soon as practicable. If a determination is made that the submitted information meets the requirements for protection, the Protected CII Program Manager or the Protected CII Program Manager's designee shall mark the information as required in paragraph (c) of this section, and disclose it only pursuant to § 29.8.

(2) If the Protected CII Program Manager or the Protected CII Program Manager's designees make an initial determination that the information submitted does not meet the requirements for protection under the CII Act of 2002, the Protected CII Program Manager or the Protected CII Program Manager's designees shall:

(i) Notify the submitter of the initial determination that the information is not considered to be Protected CII. This notification also shall:

(A) Request that the submitter further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002;

(B) Advise the submitter that the Protected CII Program Manager or the Protected CII Program Manager's designees will review any further information provided before rendering a final determination;

(C) Provide the submitter with an opportunity to withdraw the submission;

(D) Notify the submitter that any response to the notification must be received by the Protected CII Program Manager or the Protected CII Program Manager's designees no later than thirty calendar days after the date of the notification; and

(E) Request the submitter to state whether, in the event the Protected CII Program Manager or the Protected CII Program Manager's designees make a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of

in accordance with the Federal Records Act.

(ii) If the Protected CII Program Manager or the Protected CII Program Manager's designees, after following the procedures set forth in paragraph (e)(2)(i) of this section, make a final determination that the information is not Protected CII, the Protected CII Program Manager or the Protected CII Program Manager's designees, in accordance with the submitter's written preference, shall maintain the information without protection or following coordination, as appropriate, with other Federal national security, homeland security, or law enforcement authorities, destroy it in accordance with the Federal Records Act unless the Protected CII Program Manager or the Protected CII Program Manager's designees, consistent with the coordination required in this subpart, determine there is a need to retain it for law enforcement and/or national security reasons. The Protected CII Program Manager or the Protected CII Program Manager's designees shall destroy the information within thirty calendar days of making a final determination. If the submitter, however, cannot be notified or the submitter's response is not received within thirty calendar days after the submitter received the notification, as provided in paragraph (e)(2)(i) of this section, the Protected CII Program Manager or the Protected CII Program Manager's designee will destroy the information in accordance with the Federal Records Act, unless the Protected CII Program Manager or the Protected CII Program Manager's designee, after coordination with other Federal national security, homeland security, or law enforcement authorities, as appropriate, determines that there is a need to retain it for law enforcement and/or national security reasons.

(f) *Changing the status of Protected CII to non-Protected CII.* Once information is validated, only the Protected CII Program Manager or the Protected CII Program Manager's designees may change the status of Protected CII to that of non-Protected CII and remove its Protected CII markings. Status

changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

**§ 29.7 Safeguarding of Protected Critical Infrastructure Information.**

(a) *Safeguarding.* All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times by appropriate storage and handling. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

**§ 29.8 Disclosure of Protected Critical Infrastructure Information.**

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to an employee of the Federal government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written